Utah Bureau of Criminal Identification
NEWSLETTER
Department of Public Safety

VOLUME 108:1 http://bci.utah.gov JANUARY 2008

DRIVER LICENSE PRIVACY PROTECTION ACT

Every week we hear about another misuse or security breach of personal information. The Driver License Division is committed to maintaining the privacy and security of information provided by our customers.

In 1989, actress Rebecca Shaeffer was murdered. A private investigator, hired by an obsessed fan, obtained Ms. Shaeffer's address from the California Department of Motor Vehicles. The fan used the information to stalk and to kill her. In response to this tragedy and a number of other abuses, Congress passed the Driver's Privacy Protection Act (18 U.S.C. 2721-2725).

The Driver's Privacy Protection Act (DPPA) prohibits the release and use of certain personal information from state motor vehicle records. The Act defines personal information as the photograph, social security number, driver identification number, name, address, telephone number and medical or disability information. DPPA defines the purposes under which personal information must be released and the purposes under which it may be released.

In 2000, the Act was amended to include the definition of "highly restricted personal information". Under this amendment, highly restricted information may only be released with the express written consent of the driver unless the request meets the criteria of one of four purposes.

In addition to the federal law, the Division must also adhere to Utah's Government Record Access Management Act (GRAMA). GRAMA defines requirements state agencies must follow when a request for information is received.

Every request for information received at the Driver License Division is reviewed. We determine if releasing the requested information falls within the parameters of the law. Prior to the release of an approved request, the requestor must complete and submit the necessary forms, which include language stating the purpose for the request, the protections and limitations on how the information can be used and the penalties for misuse. To ensure Driver License data is being accessed properly, the Division is currently reviewing all non-criminal justice requests. *At this time, criminal justice agencies are only authorized to use this data for criminal justice or criminal justice employment purposes.* During the upcoming TAC meeting, a representative from the Driver License Division will be discussing this issue further.

A full copy of the Driver Privacy Protection Act is available in the Utah Driver License section of the *BCI Operating Manual.* Please watch the BCI Newsletter, Message of the Day, and other sources for further information. More information on this issue will be covered at the 2008 TAC Conference.

ENDANGERED PERSON ADVISORIES

Please remember to call BCI when you submit an EPA transaction! The EPA transaction was written with the intention of having an extra course to take regarding missing persons rather than relying on the usual Attempt to Locate (ATL). As part of the EPA, your agency contacts BCI when you transmit the EPA and BCI forwards the data to the local media. This is sent to them as an email, not a broadcast like an AMBER Alert. Following this notification, the media can contact the agency for further information.

If the local agency fails to call BCI, the information will not get to the media! If it is not urgent enough to warrant issuing an EPA and getting the media involved, please send an ATL using a broadcast message or NLETS AM.

If you have any questions, please contact BCI at 801-965-4446

ORIGINAL OFFENSE CODE (OOC)

You're making an NCIC Wanted Person entry, or modifying an existing Wanted Person entry, and you get an error concerning the **OOC** field. Why?

The OOC field lets those who see the entry know why the individual was in custody in the first place. The OOC field can only be filled out when the Offense Code (OFF) indicates escape, probation violation, etc. The OOC field lets officers know if the wanted person they are dealing with was originally in custody for forgery, embezzlement, rape, weapons violations, homicide, etc.

Entry of an NCIC code into the OOC field is mandatory when the NCIC code in the OFF field equals: 4901, 4999, 5001, 5002, 5011, 5012, 5013, 5014, 5015, 8100, 8101, or 8102.

In a wanted person hit response, the OOC Field will be translated just as the OFF Field is translated currently. If the individual was in custody for several charges, list the most serious in the OOC field.

Remember – if you were the officer on the street, you would want to know if you were dealing with an escaped forger – or an escaped murderer!

UTAH PROTECTION ORDERS ON NCIC

Utah is now adding its protection orders to the NCIC Protection Order File (POF).

These orders are being pulled from the protective orders that the courts submit to BCI each day. Protective orders meeting NCIC standards are then forwarded on to NCIC, so that law enforcement around the country can see that Pat Doe has a protective order against him/her.

BCI encourages the courts to review the Protection Order File section of the *NCIC Operating Manual.* Courts are also welcome to contact BCI with any questions about protection orders.

Don't forget that NCIC loves numbers! If there is no numeric identifier for both the respondent ("bad person") and the petitioner (the person wanting protection) the order will **NOT** be placed on NCIC. Numeric identifiers can include the date of birth, social security number, etc. *A court case is not considered a numeric identifier.*

Only protective orders and mutual protective orders will be forwarded to NCIC. No-contact orders and ex-parte orders will not be forwarded to NCIC.

All protective orders (no-contact, ex-parte, mutual, orders for children, etc.) will be available on the statewide warrant system as they have always been. But don't forget that entities outside Utah cannot view the SWW file!

BCI has begun sending out notifications to courts that submit protection orders without enough mandatory information. If you receive such a notification, please remove the protection order from SWW, obtain the missing information, and add the order back on to SWW.

Please keep in mind that your actions have national ramifications. If you properly submit all necessary information, your protection order may prevent an unqualified person from purchasing a firearm in New York. Your high-quality protection order may also help local law enforcement if a respondent follows a petitioner to a family reunion in Wyoming.

UNSUPERVISED SUPPORT PERSONNEL AND BCI "RIGHTS OF ACCESS"

UCJIS AGENCIES: FBI policy requires your unsupervised support personnel undergo a fingerprint background check. So you can send them to BCI to get a Right of Access, and you've done your job, right?

Unfortunately, for you, no. A BCI "Right of Access" only shows what (if anything) shows on the individual's *Utah* criminal history. Information from other states is not disseminated during a "Right of Access." In theory, an individual can have arrests in all other 49 states, but if he/she has never been arrested in Utah, that person's Utah "Right of Access" will show no record!

FBI policy requires a national fingerprint based background check on all unsupervised support personnel. If your agency has unsupervised people in your building, you must submit a 10 print card on each person, along with a "Fingerprint Submission Form." These can be mailed (in the same envelope) just as you would mail in the fingerprint card for a new UCJIS operator. (When you initially run the individual, use Purpose Code "C.")

".stat REPORTS"

COURTS: – do you ever check out your ".stat" reports? What are the stat reports, what do they mean, how can they help you, etc.?

Most courts can obtain these reports from the FTP server like you would get your Auditing or Booking Report. The file name will contain your Court ID and the date of the submission: a report from court J3030 who made their submission on December 3, 2007 would have the file name of "J3030WARR1203_200712032040.stat."

The report explains what happened with each disposition and warrant that was added/modified/recalled with that day's submission. It will give the Court ID, the warrant number, and what happened to the warrant. Was the warrant added, was the warrant recalled, did some error prevent the warrant from getting added to SWW?

Did the disposition get added to UCCH? Or was there a problem?

At the end of the report is a short summary of that submission's results. Some of the information includes: Additions, Modifications, Cancellations, Recalls, Rejections, and other information.

A sample ".stat" report can be seen on the last page of this newsletter.

Please take the chance to review your court's reports as often as possible, and make any necessary changes to warrants or dispositions.

BACKGROUND CHECKS ON LOCAL AIRPORT PERSONNEL

BCI audits have found agencies running UCCH or III backgrounds on individuals who work at the local airport. However, this is a violation of BCI and NCIC policy, as this is not a "criminal justice" purpose.

Such individuals can undergo a background check through the Transportation Security Administration. Please contact Janet Glaittli at 801-575-2204 for questions about these TSA checks.

KEEPING YOUR INFORMATION SECURE?

WASHINGTON (CNN) - About 140 foreign intelligence organizations are trying to hack into the computer networks of the U.S. government and U.S. companies, a top counterintelligence official said.

Joel Brenner, the national counterintelligence executive, told CNN "We get intrusions from all point of the compass. It is really misleading to focus on one country," he said. "They are coming from everywhere now. It is a pervasive problem."

Because it's easy for hackers to disguise where an attack originates, Brenner said, the best course of action is to tighten up one's own networks rather than to place blame. The nation's electronic systems are too easy to hack, and the number of world-class hackers is "multiplying at bewildering speed," he said.

Brenner warned that hackers could create chaos by manipulating information in electronic systems the government, military and private industry rely on. The coordinated cyber attack launched against Estonia last spring will not be the last one against a nation state, he said. "We had better heed the warning. We have got to do a better job of protecting our networks and thwarting adversary cyber intrusions."

Brenner said the matter is getting serious attention at the highest level of the federal government.

RICHFIELD FAILOVERS AND DLD DATA

When UCJIS information is being run off of the Richfield Failover Server, please keep in mind that any Utah driver license information received may not be completely up-to-date.

Unlike some other UCJIS files, which update several times a day, the driver license information updates once each morning. If we are on the Richfield Server, the driver license information will become more outdated as the day goes on. Thus, an individual's driver license information on UCJIS may show his license is valid, when it has actually been suspended since the failover took place. Fortunately such instances will be infrequent, but please keep this information in mind.

IDENTITY THEFT VICTIMIZED AT WORK?

ID Thieves Don't All Use Digital Methods - Analysis shows 20 percent of incidents happened in workplace

HACKENSACK, N.J. - A review of Secret Service files has found that only half the cases of identity theft involved technological devices, such as computers, scanners and digital cameras, and only 10 percent were done exclusively through the Internet.

In a fifth of the other cases, thieves stole personal data the old-fashioned way.

Low-tech tactics included rerouting mail by sending change of address requests to institutions handling credit card and bank accounts, swiping items right from residents' mailboxes, and "Dumpster diving" - going through trash for information used to produce counterfeit documents and to open credit accounts.

Researchers analyzed 517 closed Secret Service cases of ID theft from 2000 to 2006. It was the first study of such files from the federal agency, which is responsible for investigating identity theft and fraud.

Among the findings:

A fifth of the time, identity thieves stole personal data at their workplace. Of them, 60 percent were employed in the retail industry - stores, car dealerships, gas stations, casinos, restaurants, hotels, hospitals and doctors' offices. An additional 22 percent worked for financial services, such as banks and credit-card companies, and *9 percent were in government.*

ID Thief?

People were victimized by a family member or friend 16 percent of the time. Personal information was stolen from someone's home, car, wallet or pocketbook 12 percent of the time.

The study follows a recent Consumer Reports poll that found Americans overwhelmingly believe they are more vulnerable to identity theft when a business has their Social Security number. Most respondents said they want companies to stop using the numbers to identify customers.

A Social Security number, coupled with your date of birth and address, is the Holy Grail for identity thieves, said Cindy Wofford, special agent in charge of the Secret Service's Newark field office.

"Those three things together identify you," she said, adding you should never give out personal information over the telephone or Internet unless you know whom you're dealing with.

Consumers have become more savvy to Internet scams meant to trick them into divulging account numbers, passwords and other personal information. They know all about the Nigerian advance-fee scheme. They may have become less vigilant about other tactics, authorities say.

Lynch urged people not to give their Social Security numbers when filling out any type of medical forms or applications.

"Certainly consumers are much more at risk now for having their information compromised than in the past, either by electronic, online or the low-tech means," said Reagan. "Just as in the real world, when you walk out of your house and you have to be watchful, careful and cognizant of your surroundings, that doesn't differ when it comes to your personal information.

"It can become ruinous if it's in the wrong hands."

By Peter J. Sampson - The Record (Hackensack N.J.)

NEW LEO ONLINE APPLICATION

A new online application is a recent enhancement that enables current LEO members to facilitate the application process for co-workers. Click on the hyperlink located on the left column of the homepage to access the new, fillable online application. (Of course, the paper application can still be faxed to LEO Member Services.)

Simply type in the required information and hit the submit button. The LEO system will securely transmit the application through an encrypted tunnel to LEO Members Services with the purpose of starting the vetting process. After hitting the submit button, the FBI Rules of Behavior form will be displayed. This form must be read, understood, and signed by all applicants. Fax the form to LEO Member Services at 877-232-9536. This form must accompany the online application in order for LEO Member Services to complete the application process and activate a new LEO account.

US POLICE FATALITIES 2007

By MATT APUZZO

WASHINGTON (AP) - A record number of fatal traffic incidents and a double-digit spike in shooting deaths led to one of the deadliest years for law enforcement officers in more than a decade.

With the exception of 2001, which saw a dramatic increase in deaths because of the Sept. 11 terrorist attacks, 2007 was the deadliest year for law enforcement since 1989, according to preliminary data released jointly by the National Law Enforcement Officers Memorial Fund and Concerns of Police Survivors.

The report counted the deaths of 186 officers as of Dec. 26, up from 145 last year. Eighty-one died in traffic incidents. Shooting deaths increased from 52 to 69, a rise of about 33 percent.

"Most of us don't realize that an officer is being killed in America on average every other day," said Craig W. Floyd, chairman of the National Law Enforcement Officers Memorial Fund.

Historically, officers have been more likely to be killed in an attack than to die accidentally and shootings outnumbered car crashes. But those trends began to reverse in the late 1990s. This year, about six of every 10 deaths were accidental.

Floyd credited technology improvements with helping reverse the trend. Safety vests save lives and non-lethal devices such as electric stun guns prevent some fatal encounters, he said. He attributed the spike in shooting deaths to the increase in violent crime nationwide.

Of the 81 traffic deaths this year, 60 officers died in car crashes, 15 were hit by cars and six died in motorcycle crashes.

Police departments have worked to limit high-speed chases and only seven of the car crashes were attributed to such pursuits, Floyd said. Crashes involving a single police cruiser responding to a call were far more common, he said.

Texas led the nation with 22 fatalities followed by Florida (16), New York (12), and California (11).

Domestic violence and traffic stops were the circumstances that most commonly led to fatal police shootings this year, the report found.

The average age of officers who died in 2007 was 39. Most were men and had served an average of about 11 years in law enforcement.

Summary from The Associated Press . USA, 12/27/07

UCR/NIBRS REMINDERS

Our next Basic NIBRS Training will be held in the BCI Training Room on Thursday, April 10th (9am-5pm).

For information, please contact Della Riquelme at 801-965-4454.

MISSING PERSONS

NCMEC WEBSITE

ARE YOU USING THE NCMEC WEB SITE TO ITS FULL POTENTIAL?

Visited the website for the National Center for Missing and Exploited Children (NCMEC) lately? If not, you're missing out on valuable information for your agency, community, and family.

LAW ENFORCEMENT: Click here for training materials that can be ordered or downloaded for free. This page also covers the Netsmartz program, and has model policies for handling missing or exploited children.

PROSECUTING ATTORNEYS: Click here for information developed especially for attorney's offices. Information available includes dealing with international abductions, state resources, state custodial statutes, federal statutes, legal resources, and a pamphlet about having children testify in court.

ALL AGENCIES: Information for families and parents can be found here. Please use this information at every opportunity. (You may want to place a link on your agency's web site!)